RESEARCH ARTICLE OPEN ACCESS

Awareness of cyber laws - A Review

Bhargav Raj S[1], Edwin Raj D[2]
[1] Scholar, Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027, India.
[2]Scholar, Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027, India.

Abstract:

The cybercrime is the most described for the criminal activities. Cybercrime are the common practices of an computer expert, these activities are taken place by the criminals to steal others Documents, Hack accounts, Destroying Network and for Transferring money to there accounts. The cybercrime include illegal activities like Data interference, System interference, Forgery and Electronic frauds, e-mail abuse, hacking of accounts.

Cyber laws is used to describe the issues related to the communication technology. Similarly cyberspace is the distant field law in the way the properties or contents of many legal fields including intellectual property, Privacy, Freedom of expression. Cyber law is an attempt to design the low for the physical world, the activities that taken place in the internet by the humans. Cyber law as a major impact in the activities and it covers a large platform of the cyberspace [1].

Cyber law is an legal system that deals with internet, cyberspace, and the respective issues. It covers a large area, encompassing several topics and there subtopics including freedom of expression, access to and usage of internet, and online privacy. Cyber law can also be referred as the low of internet.

The IT Act, 2000 as amended by the IT (Amendment) Act, 2008 is known as the cyber low. In the chapter XI entitled "Offences" in which cybercrime have been declared as penal offences punishable with imprisonment and fine. The IT Act of 2000 have many positive aspects. It also allow us to know the important issues of security [2].

Keywords— **Cyber Space, Cyber Crimes, Technologies, Laws amended, Networking.**

I. INTRODUCTION

Cyber Law is the law governing the cyber space(Internet). It is a very wide term included in computers, networks, software, data storage devices , in Internet, websites, emails and even electronic devices such as mobile, ATM machines.

Cyber Law encircles the rules of guide:

- Which has been approved by the government.
- Which have to be followed by certain territory.
- Which has to be obeyed by all persons on that territory.
- Violating these rules could lead to government action such as imprisonment

(or) fine (or) to pay a certain amount of composition [2].

Cybercrimes can be encircled related to:

Cyber-crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in e-commerce and online share trading has led to a phenomenal gush in incidence of cyber-crime. Cyber crime are the illegal activity the Department of Justice divides the cyber-crime into three categories. Computer used as a target device to gain the network access, computer used as a weapon to launch the denial of service, computer used as accessory to store the illegal data.

Electronic signatures are used to authenticating electronic records. Digital signatures are one of the electronic signature. Digital signatures satisfy three major legal requirements that is, signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

Intellectual property is referred to creations of the human mind a story, a song, a painting, a design and so on . The facets of intellectual property that related to cyber space are covered by the cyber law. Cyber law in relation to computer software, computer source code, websites, mobile phone, network access, data content.

Data protection and privacy laws aim to achieve a real balance between the privacy of the individual and the interests of data controllers like banks, hospitals, email service provider. These laws seek to address the challenges to provide privacy collecting, storing and transmitting data using the present technologies.

Needs of cyber law:

- Cyberspace are difficult to govern and regulate using conventional law.
- Cyberspace has complete disrespect for jurisdictional boundaries. Because hacker from India could break into a bank's electronic vault using a computer in abroad and transfer millions of Rupees to another bank to another country, all within minutes. The hacker just need a laptop (or) a computer and a cell phone to hack into the account.
- Cyber space is a gigantic area of networking where every second, millions of e-mails, fax, and messages are been transferred around the world, even billions of transactions are being done in the world.
- Cyberspace offers enormous potential for anonymity to the people. Information are Readily available with encryption software and concealing tools that smoothly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.
- The law of real world cannot be interpreted in the emerging cyber space to include all the aspects of the cyberspace.
- Internet requires an supporting legal infrastructure as the time moves in the technology [3].

However substantial legal questions have been arisen in many context. The digital medium provides security or shield's to the anonymity and fake identity profiles. In the recent survey made by the experts it shows that there are numerous internet users receiving unsolicited emails which contain obscene languages and harassment. The cyber-stalking takes place to those people who put there individual profile information on the social media.

II. History or Origin of cyber laws.

The primary source of cyber law in India is the Information Technology Act, that is the IT Act of 2000 (17 October 2000) . IT (Amendment) Act, 2008 is known as the cyber low. The primary objective of the Act is to provide legal recognition to e-commerce and to facilitate filing of electronic records with the Government. The IT Act also introduced various cyber-crimes and provides strict punishments and also fine to be payed.

On the same day, the Information Technology Rules, 2000 also came into force. These rules tells the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.

There are more than 57 laws that are amended in India. There are more 27 offences(illegal act) that include sexual abuse, violation of privacy, Cyber terrorism, Hacking with computer systems , Data Alteration, decryption of any information through any computer resource, Un-authorized access to protected system, Publishing False digital signature certificates etc. all the crimes are amended and the person who is caught doing this criminal activity will be punished based on the jurisdiction specified in the law book. In Sec 78 of IT Act there are 24 laws which are been empowered by the police authority under the IT Act. There acts are like Sending threatening messages by e-mail, Bogus websites, Cyber Frauds, Making a false document, Forgery for purpose of cheating, Criminal intimidation by an anonymous communication, Online Sale of Drugs and Arms etc. All the Acts of IT are punished in the IPC section.

In the modern world Inventions, discoveries and technologies are been widen. As the technologies widen the challenges in the legal world also increases. These changes is a challenge to the jurisprudence in dealing with and the business that we do. Throughout the world the courts are dealing with new challenges. The IT Act of 2000, it seeks a remedy for most of the problems. It also amended various other Acts. The Indian Penal Code 1860, The Indian Evidence Act 1872, The Banker's Book Evidence act 1891, The Reserve Bank of India act 1934.

The cyber-laws and there punishment are

1. **Penalty for damage of computer system:**
   - If any person without permission of the respected owner downloads or extracts any database, introduce virus in the computer system, changes the account of a person and tampering the computer system, misusing of the data etc
   - The penalty that is laid on the person who illegally misused the computer system and damaged are fined to pay 10,00,000 to the person who is effected by the loss of the damage.
2. **Penalty for failure to furnish I formation, return:**
   - If a person fails to provide a furnish document or report to the certified authority, he/she will be liable to the penalty of Rs. 1,50,00/- for each failure like those.
   - If any book or record or not provided in a specific time period, he/she will be liable to the penalty of Rs. 5,000/- per day.
   - If a person fails to maintain the books, accounts or records which is under is control, he/she shell be liable to a penalty not exceeding Rs.10,000/-for every day.
3. **OFFENCES:**
   - Tampering a computer source code or document.
   - Penalty of Rs.2,00,000/-
   - Hacking

- Penalty of Rs.2,00,000/-. Plus 3 years of jail

4. **Protection System**
   - Computer system or computer network can be declared as protected by the government. If any person attempts to hack or tamper he shall be imprisoned for 10 years and with certain amount of fine.
5. **Penalty for misrepresentation:**
   - If a person makes mistake in the licence or digital signature certificate, he shall be imprisonment and with fine or both.
6. **Penalty for breach of confidentiality and privacy:**
   - Access to document, records, information, books etc. are transferred to others without the permission of the concerned person will be imprisoned and fine worth one lakh.
7. **Penalty for publishing digital signature certificate false in certain particulars:**
   - Publish of digital signature or publish to any other person with knowledge, shall be punished with imprisonment up to one lakh of fine**.**
8. **Publication for fraudulent purose:**
   - If a person publish or creates a digital signature for fraudulent transaction purpose, shall be imprisonment and fine up to one lakh.

The Information Technology (IT) Act of 2000 any offence that are committed our side the India (sec. 75). This act shall be applied to only those who committed offence outside the India irrespective of his nation[4].

- ✓ Sec. 76 Confiscation.
- ✓ Sec. 77 Penalties or confiscation not to interfere with other punishment.
- ✓ Sec. 78 power to investigate offences.
- ✓ Sec, 79 Network service providers not to be liable in certain cases.
- ✓ Power of police officer and other officers to enter search.
- ✓ Sec. 81 Act to have overriding effect.
- ✓ Sec 81A Application of the Act to electronic cheque and truncated cheque.
- ✓ Sec. 83 Power of give directions.
- ✓ Sec. 84 Protection of action taken in good faith.
- ✓ Sec. 85 Offences by Companies.

III. Literature Review

Title of paper: Cyber law

Name of the author: Taraq Hussain Sheik

According to the paper presented "Cyber space is an ever changing process and it should fit itself to the call of time. Expansion of the internet world gives rise to numerous of illegal issues with these rapid growth the author suggests that the enforced cyber law should be renewed timely to suit the crimes committed .The liberal interpretation of the judgement should be based on practical experience and the wisdom of judgement should be found in the existing scenario of the cyber space crime. The internet should be enabled with supporting legal infrastructure and should be in tune with times .The enactment of Cyber Law is relevant according to the traditional infrastructure and has failed to enact the cyber law to the E-Commerce, and to the other biggest future of the internet and these should be revised according to the vibrant growth [4].

Review 2:

Title of paper: Legal Implication of the Cyber Crimes

Name of the author: Nikita Barman

According to this paper presented "The information act i.e the IT world differentiates the Cyber Crimes into Cyber contraventions and Cyber crimes .Making Cyber Space network more secure requires sophisticated system and

outsmarting intellectual personalities .The vague and ambiguous laws should be interpreted liberally according to norms in the society .The tools that are available for hacking ,spamming and breaking into secure network should be traced and made useless .The information and knowledge regarding the cyberspace network should be available in limited editions [6].

IV. PROBLEM: Problems of Cyber Law

There are crimes which are not investigated and which are investigated by the SOCA. At the present world the electronic crime(e-crime) has become more and it is very complicated to the regional police force to fine the hackers or the person who is doing all the illegal activates in the state or nation.

1. Level of work: Serious Organised Crime Agency(SOCA), takes the help of the regional police force to undertake the operation of finding the person who is undertaking the illegal activity.
2. Modern technology: as the modern world develops the technologies will also develop with advance features in it.
3. Measurement of e-crime in Nation: As the cyber space is vast it is little difficult to measure the e-crimes that are happening around us.
4. Acceptance of e-crime: The acceptance level of e-crime won't be the same because the SOCA (serious Organised Crime Agency) and CEOP (Child Exploitation and online protection Centre) are the two serious crimes. Which ore most investigated? Regional force cyber-crimes are not so seriously undertaken and actions are taken to overcome these problems.
5. Rapid development of telecommunication and global development of computer network.
6. Theft of source code and access to the passwords.
7. Hackers attacks.
8. E-mail thefts.
9. Tampering of the documents.
10. Fraud and forgery [5].

V. Suggested ideas

As my concern the government and the jurisprudence court of counsel has to take a proper measure and lay an strong and effective law, saying that the person who is doing a illegal activity on the cyber space will be commenced a strict rules and they will be punished.

The court should lay a laws more effective than the previous laws made by them, because of the rise in the criminal in the cyberspace (internet). The rise of cyber criminals should be reduced because present generation is the field of internet and the networking where more of online transaction takes place around the world.

All the web sites and social web sites should contain a section regarding, the rules and regulations regarding the cybercrime and there punishments for doing the crime, if any person is doing any illegal activity knowing after the rules and the jurisprudence laws. Even after that if the person dose so he will be servilely punished and also has be pay a certain amount of money to the court.

VI. Objective: Cyber Law Objectives

a. The amended acts should be rescheduled based on the modern technology.

b. To guide the people about there legal laws of using the cyberspace (internet).

c. The web sites should contain more awareness on the issues of illegal activate.

d. The social sites should hide the personal information of the person so that it won't be visible to the anonymous people for mis-using it.

e. Safe transaction and shopping should be done online by safeguarding the bank account number and the password.

f. Should create awareness about the newly amended laws to the people.

g. Login details and passwords in the mobile and computer systems should be secured.

h. Effective software and hardware has to be developed based on the modern technology.

VII. Conclusion

As the modern world grows and the technology improves the cyber criminals will as adopt to the modern grown technology. The cyber laws has to be re-written (or) should be altered based on the changing technologies. The corporate and other companies also so adopt to these changes because of the increase in the cyber-crime. The company should not only be aware of the law but also should implement a hardware and software which is best suited to the modern technology.

The awareness of the cyber laws and the crimes has to be thought in the schools and the colleges so that the students will also have a knowledge of what are the cyber laws and the cyber-crimes. This is the responsibility of the respected intuitions to educate the students about these laws.

The laws as to change for the betterment of the mankind, and also the laws won't be static that is same throughout it will be changing as the time passes.

VIII. REFERENCES

[1] CYBER LAW & INFORMATION TECHNOLOGY Talwant Singh Addl. Distt. & Sessions Judge, (Delhi) http://CYBER-LAW-AND-INFORMATION.COM

[2] CYBER LAW AND INFORMATION TECHNOLOGY R. M. Kamble International Journal of Scientific & Engineering Research, Volume 4, Issue 5,(May-2013) https://www.ijser.org/researchpaper/CYBER-LAW-AND-INFORMATION-TECHNOLOGY.pdf

[3] Cybercrime law(and the problems of police enforcement) Denesh Edgar Nevill Chair, BCS Cyber Crime Forensics SG 2009 http://www.cybercrime-law-problems/denevill-070409.pdf

[4] Cyber Law: Provisions and Anticipation(Taraq Hussain Sheakh) http://www.researchgate.net/profile/Drtariq Sheakh/publication/231188141

[5]Cyber Law Provisions and Anticipation/Links/0912f5065cc3dds2a3000000/cyber-Law-Provisions-and-Anticipatio.pdf

[6]Legal Implications of Cyber Crimes on Social Networking Websites (Nikitha Barman) http://www.ijsrp.org/research-paper-1215/ijsrp-p4850.pdf

[7] Cyber Crime And Law (Dhawesh Pahuja) (july 17, 2011) Bnhgalore http://www.legalindia.com/cyber-crime-and-the-law

[8] "Cyber Crime against Individuals in India and IT Act"(Vshal Dhotre) http://www.shodh.inflibnet.ac.in